

1 issue my ruling on the motion to suppress.

2 (At 9:23 a.m., a recess was taken until 9:35 a.m.)

3 THE COURT: Thank you. Please be seated. I note the  
4 presence of counsel, presence of the defendant.

5 The Court is required in viewing the motions to  
6 suppress to note first that this is a motion to suppress  
7 information obtained from a search warrant that was executed  
8 on the apartment residence of the defendant. Where a search  
9 warrant has been used, the burden falls upon defendant to show  
10 a constitutional infirmity in the issuance of that warrant.  
11 See *United States v. Esser*, 441 F.3d 1109 at 1112, Tenth  
12 Circuit 2009.

13 The Constitution requires that before a warrant is  
14 issued, probable cause must exist where attending  
15 circumstances would lead a prudent person to believe there is  
16 a fair probability that contraband or evidence of a crime will  
17 be found in a particular place. In assessing whether there is  
18 probable cause for a warrant, the Court assesses the  
19 sufficiency of a supporting affidavit based on the totality of  
20 the circumstances. Further, a Magistrate or a Judge's  
21 determination that a warrant is supported by probable cause is  
22 entitled to great deference.

23 On review, the Court's task is to ensure that the  
24 Magistrate had a substantial basis for concluding probable  
25 cause existed. That's *United States v. Perrine*,

1 P-E-R-R-I-N-E, 518 F.3d 1196 at 1205, a Tenth Circuit 2008  
2 decision.

3 The Court will also note with regards to the good  
4 faith exception, the Court will presume the officer acts --  
5 actions of the officer to be objective and in good faith when  
6 supported by a warrant. The presumption is not absolute,  
7 however, and can be overcome by demonstrating that a warrant  
8 was based on an affidavit so lacking in indicia of probable  
9 cause as to render official belief in its existence entirely  
10 unreasonable. See *Leon*, 468 U.S. at 923.

11 Reliance is entirely unreasonable only if the  
12 affidavit submitted in support of the warrant is devoid of  
13 factual support. See *Cardall*, C-A-R-D-A-L-L, 773 F.2d 1128 at  
14 1133, a Tenth Circuit 1985 decision.

15 An affidavit has enough factual support to justify  
16 reliance if it establishes a minimally sufficient nexus  
17 between the illegal activity and the place to be searched.  
18 See *United States v. Gonzales*, 399 F.3d 1225, 1230 to 31; and  
19 see *United States v. Henderson*, 595 F.3d 1198 at 1201  
20 through 1202. And that's H-E-N-D-E-R-S-O-N.

21 The Court finds that first there is -- applying the  
22 standard as required, there is probable cause to support the  
23 issuance of the warrant in this matter. The test is not  
24 whether evidence exists or whether the particular defendant  
25 knew that what he was doing constituted the download of child

1 pornography. The test is whether there is a fair probability  
2 that evidence of a crime will be found in a particular place.

3 Based upon the affidavit and the experience and the  
4 knowledge and training of the affiant, he was aware of certain  
5 networks that operate and the particular ways by which they  
6 operate. The information indicates and the affidavit notes  
7 that this particular network upon which he was operating has  
8 been found to be a significant -- well, it is not found to be  
9 a significant source of music or adult pornography or  
10 theatrical movies or copyright material but rather, because of  
11 the way that it operates, has been a source of persons of  
12 which to collect or share child pornography files. So we are  
13 operating on a network that is known to be a source based upon  
14 the way it operates for operation by individuals who seek to  
15 collect and/or share child pornography.

16 There is specific means by which the individual gets  
17 to operate or is allowed to operate on that network and  
18 obtains keys from users and bulletin boards. And I'm looking  
19 at paragraph P. The files or portions are uniquely identified  
20 on the targeted network by what is known as a key. The key is  
21 a sequence of alphanumeric characters and uniquely identifies  
22 the files or a portion of the file throughout the network.

23 As I read the next sentence, "Because of encryption,  
24 persons operating computers with stored locks are likely not  
25 to know the content of the block being stored on their

1 computer," but in this case we are looking at a person  
2 operating on the network who is seeking that particular block  
3 or section of a file known to contain child pornography. So  
4 while it may have been encrypted on someone else's computer,  
5 the fact is that the key that he uses seeks out or that  
6 someone uses seeks out to obtain a known child pornography  
7 file.

8 In addition, the other paragraph notes that "Your  
9 affiant knows from training and experience that someone  
10 requesting blocks of a file has taken substantial steps to  
11 install software to operate on the targeted network and  
12 additional steps to locate the key in order to facilitate a  
13 download of that block. The network provides no search  
14 mechanism to other file sharing systems, and a subject  
15 desiring to download a file must first find the keys  
16 associated with the file, such as on a website or message  
17 board."

18 Again, to the extent the individual got the wrong key  
19 number or someone provided him an email with a key that was  
20 wrong, that's a defense potentially to the ultimate charge.  
21 But it's not a defense to the probable cause that evidence of  
22 a particular crime existed on that particular computer  
23 connected to that particular IP address because of that key  
24 that was used. And in this case there were three different  
25 times that keys were used which appeared to originate from a

1 computer on that IP address as assigned to 760 Landmark Drive,  
2 Unit 603G that was requesting child pornography files that had  
3 been logged by way of the prior efforts of law enforcement to  
4 identify the particular file keys or keys associated with  
5 known child pornography.

6 So what I garner and what I see that the -- a  
7 reasonable person, prudent person, including the Magistrate  
8 Judge or Judge Christensen in this matter, is that based upon  
9 the training and experience of this officer or this agent, he  
10 identified three different downloads initiated or appeared to  
11 initiate from the computer connected to the IP address  
12 assigned to unit 603G on Landmark Drive. Those files were  
13 known based upon information.

14 And that's where the SHA values come in, where the  
15 keys probably come in, that those are in the database. And  
16 there are two different databases probably; we have the SHA  
17 database and we have the keys in that particular network, dark  
18 network, or I think Free-something or other that was  
19 referenced by Mr. Nachbar.

20 But there's two different keys that I see. One's a  
21 key to request that particular file, and then there's a key or  
22 SHA, which I would call a SHA value or hash value, that's been  
23 pegged to that file to link it to known child pornography in  
24 the database of law enforcement.

25 So in any event, we have a request being made on

1 three different occasions for what has been identified to be  
2 known child pornography files or blocks of files of known  
3 child pornography. And based upon training and experience and  
4 information known by the agent and set forth in the affidavit,  
5 the Court would find that there is probable cause to support  
6 and -- that probable cause exists based upon information that  
7 would lead a prudent person to believe there is a fair  
8 probability that contraband or evidence of a crime will be  
9 found in a particular place.

10 The next step I guess that I would see is, okay, we  
11 have a -- there may be a wireless router attached to this  
12 particular cable modem that has been assigned the IP address.  
13 And frankly, I've looked at several cases across the country  
14 that deal with IP addresses, and I have not found one that has  
15 rejected probable cause based upon the potential that there  
16 could have been a wireless device attached and operating in  
17 the area. I don't see any cases that have found that to  
18 defeat the potential probable cause.

19 But here is again the way I would look at it. There  
20 is an IP address that has been assigned to a device operating  
21 in that apartment. And maybe there is or maybe there isn't a  
22 wireless device that is extending the access, and certainly  
23 it's a good reason why we have passwords on our wireless  
24 access systems and all that. But there would be a Mac address  
25 potentially tied to that and all kinds of different things.

1 But the bottom line is -- is that that IP address was  
2 assigned to that apartment and operating out of that vicinity,  
3 and at a minimum there's fair probability that contraband or  
4 evidence of a crime would be found in that particular place.  
5 So for those reasons I don't believe that the potential that  
6 there may have been a wireless router attached to or allowing  
7 another device to access through that IP address assigned to  
8 Charter, the Internet and this particular network, defeats  
9 probable cause.

10 In addition, to the extent that there could be issues  
11 as to a lack based upon facts and circumstances, the Court  
12 would find then certainly the good faith exception would apply  
13 in this case. There is certainly enough factual support to  
14 justify reliance and establishes a minimally sufficient nexus  
15 between the illegal activity and the place to be searched.

16 And again, I see the test not being as did the user  
17 of that device at this particular time as identified in the  
18 affidavit know that they were downloading child pornography,  
19 not the test. The test is, was there a fair probability that  
20 evidence of a crime would be located on devices attached to  
21 that IP address. And the answer is yes because those files  
22 that were potentially -- that were identified and were being  
23 sought or blocks of those files were known child pornography.

24 Now, whether it was known by the user of the device  
25 that they were downloading child pornography is an issue for

1 resolution at a trial on the merits of the charges. But I  
2 would for those reasons deny the motion to suppress and direct  
3 a minute order incorporating by reference therein this Court's  
4 oral ruling be entered in this case.

5 That then brings us to the issues raised regarding  
6 the 414 evidence. And I would hear from -- I'd hear from the  
7 United States first, and then I would hear from -- ultimately  
8 there is first a determination as to whether or not this is  
9 414 evidence that falls within the scope of Rule 414 of the  
10 rules of evidence. If it is, then the next question becomes  
11 whether or not it is properly admissible under Rule 403.

12 So I'll hear from the United States. I've read  
13 through the briefs. I know that the source of the issues  
14 arise from a 2002 conviction based upon, I believe, 1998  
15 activity that occurred in Georgia and ultimately involved a  
16 five-year-old and an eight- or nine-year-old relative. I use  
17 that term loosely because I'm not certain that I know there  
18 was some nexus between the mother and the -- of the victims  
19 and the defendant in this matter. But that being said, I  
20 would hear from the parties as to the motion and 414 evidence.  
21 Mr. Forwood.

22 MR. FORWOOD: Thank you, Your Honor. May it please  
23 the Court.

24 THE COURT: Counsel.

25 MR. FORWOOD: Counsel.